UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/511,825	10/20/2004	Antti Pietilainen	59643.00507	8850

32294 7590 01/13/2009

SQUIRE, SANDERS & DEMPSEY L.L.P.
8000 TOWERS CRESCENT DRIVE
14TH FLOOR
VIENNA, VA 22182-6212

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
01/13/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/511,825	PIETILAINEN ET AL.	
	Examiner	Art Unit	
	ELENI A. SHIFERAW	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 October 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12 and 15-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12 and 15-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims status

1. Claims 1-12 were previously pending and claims 13-14 were previously cancelled.

2. Claims 15-29 are presently added.

3. Claims 1-2, 5-10 and 12 are presently amended.

4. Claims 1-12 and 15-29 are presently pending.

5. The preliminary amendment, submitted on 05/04/2005, to the title is accepted.

6. Claim 1 has been fully considered for statutory reason and has been interpreted as statutory in light of applicant's disclosure page 4 lines 9-12. The nodes in light of the disclosure are personal computers or set-top-boxes. Therefore "a plurality of communication nodes" are interpreted as hardware.

Information Disclosure Statement

7. The information disclosure statements (IDS) submitted on 10/20/2004 and 10/13/2006 have been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

Oath/Declaration

8. The oath filed on 09/08/2006 complies with all the requirements set forth in MPEP 602 and therefore is accepted.

Drawings

9. The drawing is accepted.

Specification

10. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claim 25-29 **(as added new)** recite "A computer program product embodied on a computer readable storage medium." The disclosure is not supported by any program stored in a computer readable medium and/or applicant fails to disclose proper antecedent basis for claimed subject mater "computer storage medium" and/or "program product". Appropriate correction is required.

Claim Objections

11. Claims 26 and 28 are objected to: in line 3 of the claims wherein "the for the" should be changed to "for the".

Response to Amendments and Arguments

12. The objection to the drawings is withdrawn in view of submitted amendments on 10/14/2008.

13. The objection to the abstract is withdrawn in view of amendments submitted on 10/14/2008.

14. The amendments to the objected claims are accepted and the objection is withdrawn.

Regarding argument the references failure to disclose wherein "communication controller is further configured to change from time to time the link-level addresses allocated to each communication node and to transmit the newly allocated link-level address to a respective

communication node in an encrypted form" as recited in claims 1 and 12, remark pages 17 and 18 last paragraphs, and page 20 par. 4, page 21 last paragraph, page 23 paragraph 1, argument is not persuasive because Lyle discloses a system that gets an indication when change of port/IP address is needed or **when the port/IP address is not secure**, changes the port/IP address at random interval determined by pseudo-random number generator, generates a new port/IP address randomly, and sending the new and randomly generated port/IP address (see col. 30 lines 8-55 and fig. 19) that reads on communication controller being arranged to change from time to time the addresses allocated to each communication node and transmit the newly allocated address to the respective node, as disclosed on page 4 of the office action. Sufficient motivation to combine Lyle is provided on page 5 of the last office action. As disclosed on page 5 of the previous office action Nikander is applied for teaching of encrypting/hashing one or more components/link layer address of an IP address and transmitting encrypted/hashed to secure the IP address (see Nikander col. 6 lines 16-col. 7 lines 7 and col. 5 lines 24-29). Sufficient motivation to combine Nikander is provided on page 5 of the last office action.

Regarding argument the references failure to disclose "protecting a communication against someone listening in on the communication over the entire length of the communication," remark page 19 lines 17-19, argument is not persuasive because it is not claimed anywhere and also each limitation claimed is properly addressed by the office.

Claim Rejections - 35 USC § 101

15. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

16. Claims 15-19 are rejected under 35 U.S.C. 101 because they are directed to non-statutory subject matter as failing to fall within a statutory category and as being directed to software per se since the claim(s) are missing a hardware element in the body of the claim limitations. Although the preamble of the claim(s) recites "A communication controller", it does not inherently mean that the claim(s) are directed to a machine. The specification on page 7 par. 1-4 discloses that the allocating and the changing states not being hardware. Therefore claim(s) are interpreted as software per se and are not statutory since they are missing a hardware element in the body of the claim limitations to perform the steps. Appropriate correction is required.

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

18. Claims 1-7, 9 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elliott et al. USPN 5276813 in view of Lyle USPN 6886102 B1 and Nikander GB 2367986 A.

Regarding claim 1, Elliott et al. discloses a communication system (fig. 1) comprising:

a plurality of communication nodes (col. 4 lines 12-18 and fig. 1 elements "D"; *plurality of different I/O devices D*) connected by a data link (col. 3 lines 65-col. 4 lines 7 and fig. 1 elements 12-18; *data links 12-18*); and

a communication controller (fig. 1 element 10; *dynamic switch*) configured to allocate link-level addresses to the communication nodes wherein the communication nodes may be identified for communications over the data link (col. 9 lines 15-21 and fig. 9 elements 110, 112 and 115; *dynamic switch assigning link address to link-level facility*).

Elliott et al. fails to disclose wherein the communication controller is further configured to change from time to time the link-level addresses allocated to each communication node and transmit the newly allocated link-level address to a respective communication node.

However Lyle discloses changing a port IP address at prescribed random intervals (*from time to time*) by pseudo random number generator and transmitting the new changed address to receivers (see col. 30 lines 8-55 and fig. 19 element 1904) that reads on the communication controller is further configured to change from time to time the link-level addresses allocated to each communication node and transmit the newly allocated link-level address to a respective communication node.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Lyle within the system of Elliott et al. because they are analogous in a network switch/router (see fig. 1). One would have been motivated to incorporate the teachings of Lyle to confuse attackers from knowing addresses of others and preventing unauthorized access by randomly changing device addresses.

Elliott et al. attaches CRC on the packet when assigning and providing link address, as shown in col. 6 lines 52-59, for error detection but Elliott et al. and Lyle fail to explicitly disclose transmit the newly allocated address to the respective node in encrypted form.

However Nikander discloses encrypting/hashing one or more components/link layer address of an IP address and transmitting hashed (see col. 6 lines 16-col. 7 lines 7 and col. 5 lines 24-29).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Nikander within the combination system of Elliott et al. and Lyle because they are analogous in generation of address to devices. One would have been motivated to modify the teachings of Nikander to protect the address from intruders.

Regarding claim 12, Elliott et al. discloses a method for communicating data in a communication system (fig. 1), the communication system comprising a plurality of communication nodes (col. 4 lines 12-18 and fig. 1 elements "D"; *plurality of different I/O devices D*) connected by a data link (col. 3 lines 65-col. 4 lines7 and fig. 1 elements 12-17; *data links 12-18*) and a communication controller (fig. 1 element 10; *dynamic switch*); the method comprising:

allocating link-level addresses to the communication nodes wherein the communication nodes may be identified for communications over the link (col. 9 lines 15-21 and fig. 9 elements 110, 112 and 115; *dynamic switch assigning link address to link-level facility*).

Elliott et al. fails to disclose changing from time to time the link-level addresses allocated to each communication node and transmit the newly allocated address to the respective node.

However Lyle discloses changing a port IP address at prescribed random intervals (*from time to time*) by pseudo random number generator and transmitting the new changed address to receivers (see col. 30 lines 8-55 and fig. 19 element 1904) that reads on changing from time to

time the link-level addresses allocated to each communication node and transmit the newly allocated address to the respective node.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Lyle within the system of Elliott et al. because they are analogous in a network switch/router (see fig. 1). One would have been motivated to incorporate the teachings of Lyle to confuse attackers from knowing addresses of others and preventing unauthorized access by randomly changing device addresses.

Elliott et al. attaches CRC on the packet when assigning and providing link address, as shown in col. 6 lines 52-59, for error detection but Elliott et al. and Lyle fail to explicitly disclose transmitting the newly allocated link-level address to a respective communication node in encrypted form.

However Nikander discloses encrypting/hashing one or more components/link layer address of an IP address and transmitting hashed (see col. 6 lines 16-col. 7 lines 7 and col. 5 lines 24-29).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Nikander within the combination system of Elliott et al. and Lyle because they are analogous in generation of address to devices. One would have been motivated to modify the teachings of Nikander to protect the address from intruders.

Regarding claims 15, 20, and 25, Elliott et al. teaches a communication controller/method/program product for operating in a communication system (fig. 1) comprising a plurality of communication nodes (col. 4 lines 12-18 and fig. 1 elements "D"; *plurality of*

different I/O devices D) connected by a data link (col. 3 lines 65-col. 4 lines7 and fig. 1 elements 12-17; *data links 12-18*), the communication controller being configured to:

allocate link-level addresses to the plurality of communication nodes, wherein the communication nodes may be identified for communications over the data link (col. 9 lines 15-21 and fig. 9 elements 110, 112 and 115; *dynamic switch assigning link address to link-level facility*); and

Elliott et al. fails to disclose changing from time to time the link-level addresses allocated to each communication node and to transmit the newly allocated link-level addresses to a respective communication node.

However Lyle discloses changing a port IP address at prescribed random intervals (*from time to time*) by pseudo random number generator and transmitting the new changed address to receivers (see col. 30 lines 8-55 and fig. 19 element 1904) that reads on changing from time to time the link-level addresses allocated to each communication node and to transmit the newly allocated link-level addresses to a respective communication node.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Lyle within the system of Elliott et al. because they are analogous in a network switch/router (see fig. 1). One would have been motivated to incorporate the teachings of Lyle to confuse attackers from knowing addresses of others and preventing unauthorized access by randomly changing device addresses.

Elliott et al. attaches CRC on the packet when assigning and providing link address, as shown in col. 6 lines 52-59, for error detection but Elliott et al. and Lyle fail to explicitly disclose

transmitting the newly allocated link-level address to a respective communication node in encrypted form.

However Nikander discloses encrypting/hashing one or more components/link layer address of an IP address and transmitting hashed (see col. 6 lines 16-col. 7 lines 7 and col. 5 lines 24-29).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Nikander within the combination system of Elliott et al. and Lyle because they are analogous in generation of address to devices. One would have been motivated to modify the teachings of Nikander to protect the address from intruders.

Regarding claim 2, Elliott et al. discloses a communication system, wherein communications over the data link comprise an address part indicating the address of the one of the communication nodes to which the respective communication is directed and a payload part (see fig. 2-4; *a packet comprising link header field, information field, and link trailer and the link header comprising DEST ADDR, SOURCE ADDR*).

Regarding claim 3, Elliott et al. discloses a communication system, wherein the address part is not encrypted (fig. 3 elements 50 and 52; *DEST ADDR and SOURCE ADDR*).

Regarding claim 4, the combination of Elliot et al. and Lyle disclose including CRC portion see Elliott et al. fig. 4 on the message of fig. 2 but fail to explicitly disclose a communication system, wherein the payload part is encrypted. However Nikander teaches encrypting/hashing one or

more components/link layer address of an IP address and transmitting the message (see col. 6 lines 16-col. 7 lines 7 and col. 5 lines 24-29). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Nikander within the combination system of Elliott et al. and Lyle because they are analogous in generation of address to devices. One would have been motivated to modify the teachings of Nikander by encrypting the address and include the encrypted address as a payload on the data packet to protect the address from unauthorized users.

Regarding claim 5, Elliott et al. discloses a communication system, wherein communications over the data link are in the form of data packets (see fig. 2-4 and fig. 9).

Regarding claim 6, Elliott et al. discloses a communication system, wherein the communication system comprises a data distribution unit (col. 3 lines 20-33; *dynamic switch 10*) connected between the data link (*links 12-18*) and at least one external data source (*main storage*) and wherein the data distribution unit is configured to forward data from the data source to the communication nodes (*devices D*) via the data link (col. 4 lines 1-40).

Regarding claim 7, Lyle discloses a communication system, wherein the data distribution unit is further configured to forward the data to the communication nodes in a random or pseudo-random order (see col. 30 lines 8-55 and fig. 19; *generating new port IP address randomly and transmitting to receivers*).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Lyle within the combination system because they are analogous in a data routing device. One would have been motivated to incorporate the teachings of Lyle to confuse attackers from knowing addresses of others and preventing unauthorized access by randomly changing device addresses.

Regarding claim 9, Elliott et al. discloses a communication system, wherein a communication node is configured to store a link-level address allocated to it (col. 7 lines 63) and to ignore communications on the data link channel addressed to addresses other than that link-level address (col. 2 lines 65-col. 3 lines 2).

19. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Elliott et al. USPN 5276813 in view of Lyle USPN 6886102 B1 and Nikander GB 2367986 A and further in view of Laxman et al. US PG Pubs 2003/0018804 A1.

Regarding claim 8, Lyle discloses a communication system, wherein the data distribution unit is configured to transmit over the link communications addressed to an address that is not allocated to any of the nodes (Lyle see col. 30 lines 8-55 and fig. 19; *generating new unique port IP address randomly and transmitting to receivers*). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Lyle within the combination system because they are analogous in a routing switch. One would have been motivated to incorporate the teachings of Lyle to confuse attackers from knowing

addresses of others and preventing unauthorized access by randomly changing device addresses and enhance security.

However the combination fails to explicitly disclose when it would otherwise not be transmitting data to the communication nodes as interpreted in the disclosure page 7 par. 4 transmitting "when the link would otherwise be idle."

Laxman et al. discloses changing source address with a MAC address prior to sending over a network (see par. 0015 lines 10-12) and monitoring the network until the network is idle and when the network is idle transmitting the new changed MAC address (see par. 0033 and fig. 4B).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Laxman et al. within the combination system because they are analogous in data transmission. One would have been motivated to incorporate the teachings to properly transmit the packet when the network is not busy.

20. Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elliott et al. USPN 5276813 in view of Lyle USPN 6886102 B1 and Nikander GB 2367986 A, and further in view of Woundy USPN 6009103.

Regarding claim 10, one can understand that the data links 12-18 of Elliott et al., IPv6 link of Nikander are Ethernet links but the combination of Elliott et al., Lyle and Nikander fail to explicitly disclose Ethernet link.

However the examiner combines Woundy that discloses a broadband cable data distribution system (fig. 1) comprising a DHCP sever (fig. 1 element 12) for allocating network Ethernet addresses (see col. 3 lines 28-38 and col. 5 lines 17-36) to plurality of user terminals (fig. 1 element 14) connected to server via a cable modem and coaxial cable via an Ethernet type connection/Ethernet link (see col. 2 lines 60-67).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teaching of Woundy within the combination system because they are analogous in address allocating. One would have been motivated to incorporate the teachings to assign Ethernet address and enhance a security of in an Ethernet communication nodes address allocation.

Regarding claim 11, the combination of Elliott et al., Lyle and Nikander disclose all the subject matter as discloses above. One ordinary skill can understand that the addresses of the Elliott et al. and Nikander are Ethernet physical addresses but the combination of Elliott et al., Lyle and Nikander fail to explicitly disclose wherein the link-level addresses are Ethernet PHY ID addresses.

However the examiner combines Woundy that discloses a broadband cable data distribution system (fig. 1) comprising a DHCP sever (fig. 1 element 12) for allocating network Ethernet physical addresses (see col. 3 lines 28-38 and col. 5 lines 17-36) to plurality of user terminals (fig. 1 element 14) connected to server via a cable modem and coaxial cable via an Ethernet type connection/Ethernet link (see col. 2 lines 60-67).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teaching of Woundy within the combination system because they are analogous in address allocating. One would have been motivated to incorporate the teachings to allocate and enhance a security of in an Ethernet communication nodes Ethernet address allocation.

Regarding claims 16, and 21, Elliott et al. teaches a communication controller/method, further configured to transmit the newly allocated link-level addresses to the respective node (col. 9 lines 15-21 and fig. 9 elements 110, 112 and 115; *dynamic switch assigning link address to link-level facility*) in a communication comprising an address part configured to indicate a current address of the respective node and a payload part comprising the newly allocated addresses in encrypted form (see fig. 2-4; *a transmitting packet comprising link header field, information field, and link trailer and the link header comprising DEST ADDR, SOURCE ADDR that is indicating new allocated current link-level address so the device can use it as current*).

Regarding claims 19, 24, and 29 the combination teaches a communication controller method/program product, further configured to change the link-level addresses allocated to each of the plurality of communication nodes at one of random, pseudo-random, or periodic intervals (*Lyle discloses changing a port IP address at prescribed random intervals by pseudo random number generator and transmitting the new changed address to receivers* see col. 30 lines 8-55 and fig. 19 element 1904).

21. Claims 17, 22 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elliott et al. USPN 5276813 in view of Lyle USPN 6886102 B1 and Nikander GB 2367986 A and further in view of Marino et al. USPN 6026165.

Regarding claims 17, 22 and 27, the combination teaches all the subject matter as disclosed above. The combination fails to disclose the communication controller/method/program product, further configured to: allocate encryption keys to each of the plurality of communication nodes; and change from time to time the encryption key allocated to each of the plurality of communication nodes and transmit the newly allocated encryption key to the respective node in encrypted form.

However Marino et al. discloses allocate encryption keys to each of the plurality of communication nodes **(see fig. 2 element 21 and col. 8 lines 17-23; random key generator generating keys randomly and sending/allocating randomly generated keys for receiver devices)**; and

change from time to time **(randomly)** the encryption key allocated to each of the plurality of communication nodes and transmit the newly allocated encryption key to the respective node in encrypted form **(Marino et al. further discloses a data message, formed by the encoder 7 and transmitted to the receiver 6, comprises a data field 28, a device ID field 30, and a sequence number field 32, and the CRC field 34 [see col. 7 lines 14-21], the encoder 7 discloses random key generator to generate random encryption keys [see col. 7 lines 2-7 and col. 5 lines 36-39]. The data field 28 and the sequence field 32 are transmitted encrypted and the key is disclosed within the data field of the data message [see col. 7 lines 35-37 and col. 3 lines 54-61].**

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Mario et al. within the combination system because it would allow security to the data transmitted (see col. 8 lines 17-23).

Regarding claims 18, 23, 26, and 28, Marino et al. further teaches communication controller/method/program product further configured to transmit the newly allocated encryption key to the respective node in the payload part that contains a newly allocated address for the respective node (see **Marino et al. further discloses a data message, formed by the encoder 7 and transmitted to the receiver 6, comprises a data field 28, a device ID field 30, and a sequence number field 32, and the CRC field 34 [see fig. 2, and col. 7 lines 14-21], the encoder 7 discloses random key generator to generate random encryption keys [see col. 7 lines 2-7 and col. 5 lines 36-39]. The data field 28 and the sequence field 32 are transmitted encrypted and the key is disclosed within the data field of the data message [see col. 7 lines 35-37 and col. 3 lines 54-61]**.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Mario et al. within the combination system because it would allow security to the data transmitted (see col. 8 lines 17-23).

Conclusion

22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

23. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ELENI A. SHIFERAW whose telephone number is (571)272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ELENI SHIFERAW/
Examiner, Art Unit 2436

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436